UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/590,438	06/09/2000	Terence V. Trench	VISAP060	1408

22434 7590 07/27/2004

BEYER WEAVER & THOMAS LLP
P.O. BOX 778
BERKELEY, CA 94704-0778

EXAMINER	
KIM, JUNG W	

ART UNIT	PAPER NUMBER
2132	6

DATE MAILED: 07/27/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/590,438	TRENCH, TERENCE V.	
	Examiner	Art Unit	
	Jung W Kim	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *06 May 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,2,5,7-9,12-18 and 21-41* is/are pending in the application.

4a) Of the above claim(s) *13-18 and 34-41* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,2,5,7-9,12 and 21-33* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☒ Claim(s) *34-41* are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *10 May 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1, 2, 5, 7-9, 12 and 21-33 have been examined. Applicant has amended claims 1, 2, 5, 7-9 and 12, canceled claims 3, 4, 6, 10, 11 and 19, and added new claims 21-33. Amended claims 13-18 and 20, and new claims 34-41 are withdrawn from consideration for the reasons outlined below.

Election/Restrictions

2. Applicant's election without traverse of claims 1-12 and 19 in the reply filed on May 6, 2004 is acknowledged.

3. Newly submitted claims 34-41 are directed to an invention that is independent or distinct from the invention originally claimed for the following reasons: new claims 34-36 are dependent claims of the non-elected claims 13-18 and 20, and new claims 37-41 are directed to an invention drawn to the subject matter of the non-elected claims 13-18 and 20.

4. Since applicant has received an action on the merits for the originally presented invention, this invention has been constructively elected by original presentation for prosecution on the merits. Accordingly, claims 34-41 are withdrawn from consideration as being directed to a non-elected invention. See 37 CFR 1.142(b) and MPEP § 821.03.

5. Further, claims 13-18 and 34-41 cannot be entered and must be canceled by the applicant since they have been restricted or are drawn to the subject matter of the restricted claims. See 37 CFR 1.145 and MPEP § 818.01 and 818.02(a).

Response to Amendment

6. The objection to the drawings for not showing the limitation of claim 6 is withdrawn as the claim has been canceled.

7. The objections to the Specification are withdrawn as the amendments to the specification overcome the objection.

8. The objection to the title is withdrawn, as the amended title is more clearly indicative of the invention to which the claims are directed.

Response to Arguments

9. Applicant's arguments with respect to the drawings not showing the limitation of claim 5 has been fully considered and are persuasive. The objection has been withdrawn.

10. Applicant's arguments with respect to the rejections of amended claims 1, 2, 5, 7-9, 12 and new claims 21-33 under 35 U.S.C. 103(a) has been considered but are moot in view of the new ground(s) of rejection.

Drawings

11. The drawings were received on May 10, 2004. These drawings are acceptable.

Claim Rejections - 35 USC § 112

12. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

13. Claim 22 is rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention. The specification does not disclose the limitation wherein a user private key and a certificate store application on a chip card use about 2 Kbytes of memory.

Claim Rejections - 35 USC § 103

14. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

15. Claims 1, 2, 21 and 24-26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Stallings Cryptography and Network Security 2nd Edition (hereinafter Stallings) in view of VeriSign "Certification Practice Statement" Version 1.2 (hereinafter VeriSign) and Tolopka et al. U.S. Patent No. 6,044,349 (hereinafter Tolopka). As per claim 1, Stallings teaches a method of creating a digital certificate for a user comprising

a. generating a user private key and a user public key (see Stallings, page 341, 6th paragraph, last sentence; page 342, bullet 'Subject's public-key information');

b. encrypting the combination of the user public key and the set of attributes using an issuer private key to create an encrypted data set (see Stallings, page 342, bullet, 'Signature');

c. creating a digital certificate containing the user public key, the set of attributes and the encrypted data set, the digital certificate including an issuing-party identifier (see Stallings, page 342, Figure 11.3); and

d. storing the digital certificate at a user-allotted memory segment of a certificate library server (see Stallings, page 341, 1st and 2nd paragraphs).

16. Stallings is silent on the matter of obtaining a set of attributes containing data pertaining to the user and useful to an issuing party issuing the digital certificate. However, virtually all Certificate Authorities (CA) require in some fashion a means to obtain subscriber's information for creating a digital certificate. VeriSign, for example, obtains subscriber information from a securely transmitted application filed by a user requesting a digital certificate to certify a public key (see VeriSign, Section 4.2). It would be obvious to one of ordinary skill in the art at the time the invention was made to implement the step of obtaining a set of attributes pertaining to the user useful for the issuing party to issue the digital certificate in the method disclosed by Stallings. Motivation for such an implementation enables users to subscribe to the CA for the creation, storage, and distribution of a digital certificate. Further, VeriSign requires the

user private key to be securely held by the user, either by using encryption software or in a chip card (see VeriSign, sections 2.3.3 and 4.1.2).

17. Finally, Stallings teaches storing the digital certificate in a centralized location remote from the user (see Stallings, page 341, 1st and 2nd paragraphs), but does not expressly disclose storing the address of the certificate library server in a chip card. Tolopka discloses a storage and retrieval method using a chip card wherein a location/key pairing stored on a chip card enables access to the service at the location specified (see Tolopka, Figure 1; Figure 3, Reference No. 120). It would be obvious to one of ordinary skill in the art at the time the invention was made for the address of the certificate library server to be stored on the chip card since it enables the user to conveniently access content/services from the server as taught by Tolopka (see Tolopka, col. 1, line 1-col. 2, line 2). Hence, the invention covered by Stallings, VeriSign, and Tolopka further comprises:

e. storing the user private key and an address of the certificate library server on a chip card of the user, whereby the digital certificate is stored remote from the chip card.

The aforementioned covers claim 1.

18. As per claim 2, Stallings covers a method as outlined above in the claim 1 rejection under 35 U.S.C. 103(a). In addition, the method further includes the step of creating a certificate chain using the digital certificate, the certificate chain being stored in the user-allotted memory segment of a certificate library server and having a trusted

root, the trusted root being different from other trusted roots stored at the user-allotted memory segment (see Stallings, page 341, 1st and 2nd paragraph; page 342, bullet 'Issuer name'; page 349, 'Certificate Subject and Issuer Attributes'; pages 343-345, 'Obtaining a User's Certificate', especially steps 1 and 2 at bottom of page 343 and top of page 344, and Figure 11.4, 'V' node; see VeriSign, section 2.5, Figure 4).

19. As per claim 21, Stallings covers a method as outlined above in the claim 1 rejection under 35 U.S.C. 103(a). In addition, the issuing party is a registration authority, a certificate authority, a reliant party, a merchant or a service provider (see VeriSign, section 2.5.3).

20. As per claim 24, Stallings covers a certificate library server for storing digital certificate chains of users as outlined above in the claim 1 rejection under 35 U.S.C. 103(a). In addition, the certificate library server further comprises:

a. a plurality of user-specific memory segments, each of the user-specific memory segments being accessible by an address contained in a chip card of one of the users (see Stallings, page 341, 1st and 2nd paragraphs; see Tolopka, Figure 3, Reference No. 120);

b. a plurality of digital certificate chains issued to one of the users, the digital certificate chains included in one of the user-specific memory segments and each digital certificate chain being issued to the user by an issuer (see Stallings, page 342, bullet, 'Issuer name'; page 349, 'Certificate Subject and Issuer

Attributes'; page 343-345, 'Obtaining a User's Certificate', especially Figure 11.4);

c. an issuer identifier associated with each digital certificate chain that identifies the issuer on whose behalf the digital certificate is provided in the certificate library server (see Stallings, page 342, bullet 'Issuer unique identifier');

d. a user first cryptographic key included in each of the digital certificate chains, the user first cryptographic key having a corresponding user second cryptographic key being stored in the chip card of the user (see Stallings, page 342, bullet 'Subject's public-key information'; see VeriSign, sections 2.3.3 and 4.1.2);

e. a set of user attributes included in each digital certificate chain providing information regarding the relationship between the user and the issuer associated with the digital certificate chain (see Stallings, page 342, Figure 11.3; pages 348-349, 'Key and Policy Information', 'Certificate Subject and Issuer Attributes', and Certification Path Constraints'); and

f. a trusted root certificate for each digital certificate chain (see Stallings, page 345, Figure 11.4, node 'V'; see VeriSign, section 2.5, Figure 4 'VeriSign Root').

The aforementioned covers claim 24.

21. As per claim 25, it is an apparatus claim corresponding to claims 21 and 24 and it does not teach or define above the information claimed in claims 21 and 24. Therefore,

claim 28 is rejected as being unpatentable over Stallings in view of VeriSign, and Tolopka for the same reasons set forth in the rejections of claims 21 and 24.

22. As per claim 26, Stallings covers a certificate library server as outlined above in the claim 24 rejection under 35 U.S.C. 103(a). In addition, the user first cryptographic key is a user public key and the user second cryptographic key is a user private key, whereby the keys implement an asymmetric cryptographic technique (see Stallings, page 341, 1st and 2nd paragraphs; page 342, bullet 'Subject's public-key information'; see VeriSign, sections 2.3.3 and 4.1.2).

23. Claims 5, 7, 8, 12, 28-31 and 33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Stallings in view of VeriSign and Tolopka, and further in view of Hughes "Certificate Inter-operability – White Paper" (hereinafter Hughes). As per claims 5, 7 and 8, Stallings covers a method as outlined above in the claim 1 rejection under 35 U.S.C. 103(a). Stallings does not expressly disclose means for verifying the signature of a certificate. However, the steps disclosed in claim 5, 7 and 8 are typical procedures to validate a signature of a certificate. For example, Hughes teaches a simple validation routine on a digital signature which includes finding the issuer's name from the certificate and locating the issuer's public key from another digital certificate, then using the public key to validate that the certificate signature was generated by the issuer (see Hughes, page 224, 1st paragraph, steps 1-3). These steps further authenticate the pairing of the user with the certificate. It would be obvious to one of

ordinary skill in the art at the time the invention was made to apply the teaching of Hughes to the invention covered by Stallings. Motivation for such an implementation would utilize a standard and simple means of signature verification. Finally, the step of locating the issuer's public key from another digital certificate requires the step of accessing the digital certificate from the certificate library server using the issuing-party identifier (see Stallings, page 343-344, steps 1 and 2; see Tolopka, Figure 1; Figure 3, Reference No. 120). The aforementioned cover claims 5, 7 and 8.

24. As per claim 12, Stallings covers a method as outlined above in the claim 7 and 8 rejections under 35 U.S.C. 103(a). In addition, Hughes teaches that certificate library servers are typically LDAP servers (see Hughes, page 230, step 1).

25. As per claim 28, it is an apparatus claim corresponding to claims 12 and 24 and it does not teach or define above the information claimed in claims 12 and 24. Therefore, claim 28 is rejected as being unpatentable over Stallings in view of VeriSign, Tolopka, and Hughes for the same reasons set forth in the rejections of claims 12 and 24.

26. As per claims 29-31 and 33, Stallings covers a certificate store system for creating a digital certificate for a user as outlined above in the claim 12 and 24-26 rejections under 35 U.S.C. 103(a). In addition, the invention includes: the step of creating the user cryptographic key pair at a certificate authority (see Hughes, page 225, 'Centralized Generation'); a registration authority that request creation of the digital

certificate (see VeriSign, sections 2.5.3 and 4.2); and the chip card also storing an identifier of the registration authority and a software application that coordinates communication between the chip card and the certificate library server (see Tolopka, col. 3, lines 26-28; Figure 1, especially Reference Nos. 110 and 120; see also applicant's remark on page 14, 1st paragraph, 5th sentence in the amendment filed on May 6, 2004, for further interpretation of identifier). The aforementioned cover claims 29-31 and 33.

27. Claim 22 is rejected under 35 U.S.C. 103(a) as being unpatentable over Stallings in view of VeriSign and Tolopka, and further in view of Storck et al. U.S. Patent No. 5,434,395 (hereinafter Storck). As per claim 22, Stallings covers a method as outlined above in the claim 1 rejection under 35 U.S.C. 103(a). Although Stallings is silent on the matter of the user private key and the certificate store application on the chip card using about 2 Kbytes of memory, as taught by Storck, early versions of chip cards maintained only 2 Kbytes of memory (see Storck, col. 2, lines 32-33). In these chip cards, all information needed to be restricted to fit this size; further, since a larger private key enables a more secure cryptographic scheme and a more detailed application enables a more exacting profile of the user, maximizing the amount of information stored on the chip card is an obvious implementation. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made for the user private key and the certificate store application on the chip card to use about 2 Kbytes of memory, since 2 Kbytes was the storage capacity of these chip cards.

28. Claims 9 and 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Stallings in view of VeriSign and Tolopka, and further in view of Samar U.S. Patent No. 5,778,072 (hereinafter Samar). As per claim 9, Stallings covers a method as outlined above in the claim 1 rejection under 35 U.S.C. 103(a). This method does not expressly define a challenge/response authentication methodology using the user's public/private key pair with the chip card. Samar discloses such a challenge/response authentication methodology using the user's public/private key pair with the chip card (see Abstract; col. 1, lines 9-14; Figure 2, Reference Nos. 207 and 135). It would be obvious to one of ordinary skill in the art at the time the invention was made to apply the teaching of Samar to the method covered by Stallings. Motivation for such a combination enables the chip card to be authenticated using well-implemented means as taught by Samar (see Samar, col. 2, lines 53-57).

29. As per claim 23, Stallings covers a method as outlined above in the claim 9 rejection under 35 U.S.C. 103(a). In addition, the method includes the step of prompting the user for a PIN, whereby the user is verified to be the owner of the chip card (see Tolopka, col. 3, lines 35-54).

30. Claims 27 and 32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Stallings in view of VeriSign and Tolopka, and further in view of Davis U.S. Patent No. 5,970,147 (hereinafter Davis). As per claim 27, Stallings covers a certificate library

server as outlined above in the claim 24 rejection under 35 U.S.C. 103(a). The digital certificates covered by Stallings and VeriSign use public keys to authenticate the subscriber of the certificate. Although digital certificates typically certifies a public key with a user, it is well known in the art for digital certificates to generalize as means to certify any information used to authenticate a user; for example, Davis defines digital certificates as such (see Davis, col. 2, lines 47-48). Furthermore, Stallings teaches, in a different section, how symmetric keys are used to authenticate a user (see Stallings, page 239, 'Conventional Encryption'). It would be obvious to one of ordinary skill in the art at the time the invention was made for the certificates to certify a user's symmetric key. Motivation for such an implementation certifies the identity of a user as taught by Davis based on an authentication scheme simpler than public key encryption as taught by Stallings (see Stallings, page 239, 'Conventional Encryption', 1st paragraph). The aforementioned covers claim 27.

31. As per claim 32, it is an apparatus claim corresponding to claims 27 and 29 and it does not teach or define above the information claimed in claims 27 and 29. Therefore, claim 28 is rejected as being unpatentable over Stallings in view of VeriSign, Tolopka, Hughes, and Davis for the same reasons set forth in the rejections of claims 27 and 29.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP

§ 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jung W Kim whose telephone number is (703) 305-8289. The examiner can normally be reached on M-F 9:00-6:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (703) 305-1830. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Jung W Kim
Examiner
Art Unit 2132

Jk
July 9, 2004

JUSTIN T. DARROW
PRIMARY EXAMINER